	Georgia Technology Authority	
Title:	**Information Technology Reporting**	
PSG Number:	SS-08-053.03	**Topical Area:** Technology
Document Type:	Standard	**Pages:** 13
Issue Date:	March 31, 2010	**Effective Date:** 3/31/2010
POC for Changes:	GTA - Enterprise Governance and Planning Division	
Synopsis:	Requires agencies to report the status of their information security program annually to GTA.	

PURPOSE:

On March 19, 2008 the Governor issued an Executive Order taking the lead on issues of information security. This order directs GTA to issue an information security reporting (ISR) standard in March of each year requiring an assessment of the adequacy and effectiveness of information security throughout the state by defining performance measures and requiring agencies to report to GTA, the status of those measures as of the end of the current fiscal year (FY). This is consistent with GTA's role established in legislation, "To establish technology security standards and services to be used by all agencies;" (see O.C.G.A 50-25-4(a)(21). In 2009 new legislation updated GTA's powers to ". . . publish an annual state information technology report;" and can solicit reporting data from agencies up to twice a year (see O.C.G.A 50-25-7.10).

GTA will prepare and submit the annual State of Georgia Enterprise Information Technology Governance Report (ITGR) to the Governor's Office. The annual report will provide a high-level view of the state's information technology assets and projects and their criticality to the state. The report will facilitate state executives' and legislators' understanding of the current state of information technology and related risks and how each agency is performing in meeting the needs of its organization and managing those risks year to year. It will also, provide data for prioritizing and making cost effective, risk-based decisions with regards to recommended improvements.

In 2010, GTA will continue obtaining and maintaining ongoing information regarding each agency's information security program, technology assets, projects and expenditures.

While information security plans and measures are specifically exempted from public disclosure under the Open Records Act, agencies are required to strategically plan their initiatives and make these plans and corresponding performance measures or metrics available to the public.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (PS-08-005.01)

SUPPLEMENTAL EXCEPTION:

Any exceptions to this standard shall be at the discretion of and approved in writing by the State Chief Information Officer.

STANDARD

To ensure the adequacy, effectiveness, and continuous improvement of information assurance throughout the state:

1. GTA shall, in coordination with the Georgia Department of Audits and Accounts and the Governor's Office of Planning and Budget, define the performance goals and measures for the ITGR by March 31st of each year.
    a. IT performance goals and measures shall be based on specific compliance, implementation and effectiveness objectives such as but not limited to compliance with technology and security policies and standards, cost-effective service delivery, project management and mission accomplishment.
    b. The performance goals shall state a desired result of the implementation of system security and IT process requirements and the actions required to accomplish the goals.
    c. The metrics shall attempt to measure the accomplishments of each agency by quantifying the level of implementation, effectiveness and efficiency of the stated objectives.
    d. The metrics shall demonstrate progress against established objectives as technology services and security matures and shall facilitate the development of corrective actions and/or improvement plans.
2. Each agency shall conduct an annual review and report the status of its operational IT systems, applications, IT projects and information security program as of June 30th of each year.
3. Agencies shall deliver their report to GTA on or before July 31st of the same year.
4. GTA shall collect and analyze the agencies' reports and compile an annual State of Georgia Enterprise ITGR and deliver to the Governor's office by October 31st of each year
    a. The report shall provide a summary of statewide IT resources, projects and expenses as well as performance strengths, weaknesses and areas of improvement.
    b. It shall include a plan of action to improve the maturity of IT processes, governance and security throughout Georgia government.
    c. It shall also include each agency's individual report.

In addition to continuous update of each agency's IT system, application and project inventories, 2010 performance measures shall seek demonstrated progress over 2009 each agency's technology operations and project management and information security processes in the areas of:

- Security Program Management
- Business Continuity and Disaster Recovery Planning
- Incident Response and Reporting
- Security Education and Awareness
- Lifecycle Management (Enterprise Performance Lifecycle - EPLC)

See the attached appendices for current year ITGR questions and required content.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Full collection of Enterprise Security and Technology Policies and Standards

GTA's information security policies and standards are available on its website, http://gta.georgia.gov

REFERENCES

- NIST SP 800-55 Performance Measurement Guide for Information Security
- NIST SP 800-80 Guide for Developing Performance Metrics for Information Security
- NISTIR 7358 Program Review for Information Security Management Assistance

TERMS and DEFINITIONS

- **Performance Goal –** The desired results of implementing the security objective or technique that are measured by the metric

- **Performance Measures –** The actions required to accomplish the performance goal validated through the completion and analysis of the agency report.

- **Metric –** Numeric indicators used to gauge state-wide program performance and monitor progress toward accomplishing state-wide goals and objectives. Monitors and measures accomplishment of goals by quantifying the level of implementation and effectiveness

Appendix -1: Agency Profile

Contact and General Information

1. Agency Name

2. Agency Acronym*

3. To what Branch of Government does your agency belong*?
    a) Executive
    b) Legislative
    c) Judicial

4. Agency Address & Phone*

5. Agency Head Name and Contact information*

6. How is your Agency head selected*?
    a) Appointment
    b) Election
    c) Unknown

7. Does the agency have a Chief Information Officer*?
   If yes, provide CIO name and contact information

8. Does the agency have a Senior Agency Information Security Officer (SAISO)?
   If yes, provide name and contact information

9. Does the agency have a Privacy Officer?
   If yes, provide name and contact information

10. Does the agency have a Business Continuity Planner/Coordinator?
    If yes, provide name and contact information

11. Does the agency have a Project Management Office*?
    If yes, provide name and contact information

12. Is the agency identified by the Governor's executive order as an Emergency Support Function (ESF) agency?

    Note: ESF agencies are identified in the Governor's executive order (EO) and the Georgia Emergency Operations Plan (GEOP) as having primary and/or support responsibilities to provide essential services or support for those services during a man-made, natural, or environmental state emergency.

    Governor's Executive Order, "02.14.06.01 Regarding the Georgia Emergency Operations Plan", can be found at http://gov.georgia.gov/gov/exorders/2006/feb/02_14_06_01.pdf
    Please access Georgia Emergency Management Agency's website at www.gema.gov for GEOP.

13. Total number of agency employees (staff and contractor)

14. Provide all Information Technology related costs expended over the past Fiscal Year (2010) and budgeted for next fiscal year (2011) *.

Account Code	Description	FY2010 Expenditure	FY 2011 Budget
300	Personal Services		
301	Regular Operating Expense		
303	Motor Vehicle Purchases		
304	Equipment		
305	Computer Charges		
306	Real Estate Rentals		
307	Telecommunications		
309	Capital Outlay		
312	Contracts		
314	Transfers		
315	Grants		
xxx	Special Line Item Expenditure		

Information Security Program Management

15. Is your agency reporting on IT Security for itself and/or reporting on behalf of another agency?
    a) Self only
    b) Self and other (list dependent agency or agencies)
    c) Other (list reporting agency)

16. If another agency is reporting on behalf of your agency, do you have a memorandum of understanding or agreement (MOU/MOA) between your agency and the other state agency which explicitly details this arrangement?

    If yes, have you provided a copy to GTA?

17. Each reporting agency shall be categorized according the potential impact of its production or operational system(s) to the Enterprise which will be derived from the highest impact rating (high water mark) assigned to any of your production systems.
    a) High (High Impact is loss of life, severe or catastrophic adverse effect on organizational operations, assets or individuals)
    b) Moderate (Moderate Impact is serious adverse effect on organizational operations, assets, or individuals)
    c) Low (Low Impact is limited or minimal adverse effect on organizational operations, assets or individual)

18. Does your agency have a formal documented security program as required by enterprise Information Security Infrastructure standard (SS-08-005.01) [*]?

19. Select one from the options below that which ***best*** describes your agencies information security governance.
    a) Our agency adheres to the Enterprise Security Policies and Standards
    b) Our Agency adheres to the Enterprise Security Policies and Standards and augments them with internal policies to meet agency specific security objectives.
    c) Our agency has developed and maintains our own security policies and standards.
    d) Other. Please explain
    e) Our agency does not adhere to a formal security policy or governance framework.

20. Are copies of your security policies and standards readily available?
    a) Yes, via agency website
    b) Yes, via email request (internal file system)
    c) Yes, in hardcopy form only
    d) No, not at this time

21. How are agency security policies and standards communicated to agency personnel? (select all that apply)
    a) Email
    b) Bulletin/newsletter (hard or softcopy)
    c) Intranet (web) announcement
    d) Annual Security Awareness Training
    e) New Hire Orientation/On-boarding, etc
    f) Other (explain)
    g) Security policies and standards are not formally announced or communicated

Security Awareness and Education

22. How many of your agency employees (staff and contractors) completed annual security awareness training using the video produced by GTA?

23. How many of your agency employees (staff and contractors) completed annual security awareness training using agency provided materials?

24. Has your agency identified the role-based security education and awareness needs of those individuals within the organization that have unique or specific information security responsibilities?

25. Check which functions/roles have received targeted security education and training: (check all that apply)
    a) Information Security Officers
    b) Developers
    c) Application Support
    d) IT Operations Support (administrators, Help desk, etc)
    e) Network Support (engineers, administrators etc)
    f) Data Owners/Executives
    g) Other (list function/role)

26. Is record of needed or completed security training maintained and available upon request?

Business Continuity (BC) Planning

27. Does your agency have a policy requiring an actionable plan for continuing critical business processes during an emergency?

28. Has your agency identified, defined and documented the processes that achieve its core business functions?

29. Has your agency ranked the criticality of the processes that support its core business functions (those processes that MUST be performed in the event of an emergency)?

30. Has your agency identified the key personnel that are tied to each of the critical business processes?

31. Has your agency identified an alternate work site or location to conduct business in the event your primary site is destroyed?

32. Is your agency documenting BC information using the enterprise BC and DR planning tool (LDRPS) offered by GTA?

33. If you are NOT using the State's Enterprise BCP tool please identify where your BC and DR plans and procedures are located?
    a) Commercial tool (provide name)
    b) Custom developed tool (provide name)

c) MS Office or other productivity suite document (Word, Lotus, Excel, etc)
d) Hardcopy file (copy must be available upon request)
e) Ad-hoc or scramble plans

34. Select one from the options below that best describes the state of your agency's emergency preparedness.
    a) Fully documented and tested BC procedures
    b) Fully documented but NOT tested BC procedures
    c) BCP in development using GTA BCP services and support
    d) BCP in development, independent of GTA BCP services and support
    e) Ad-hoc or scramble-plans or No formal BC procedures

Security Incident Response and Reporting

35. Does your agency have a documented Security Incident Management Plan on file with GTA?

36. How many information security incident investigations were initiated this past fiscal year?
    a) How many of those investigations followed the plan?
    b) How many of the investigations uncovered a legitimate security issue?
    c) Number of legitimate incidents successfully resolved?

37. How many security investigations involved sensitive or critical systems?

38. How many incidents caused widespread or serious harm or disruption to agency operations?

39. How many incidents were reported to either GTA or law enforcement within the past year?

40. How many incidents involved breach of constituents' personal information?

41. How many constituents were notified because their confidential information had been compromised?

Appendix - 2: Production System Inventory

Agencies shall provide / update the following information for EACH production/operational system owned by the agency

42. System Name

43. System short name*

44. System's purpose

45. Select the impact categorization ratings (high, moderate, low) for each of the security objectives:

Security Objective	**Low** Impact	**Moderate** Impact	**High** Impact
Confidentiality			
Integrity			
Availability			

46. Does the system have a documented information security plan?
    a. If yes, provide name of plan
    b. If yes, what is the security plan date? (date last reviewed or updated, and approved)
    c. If yes, does the plan have considerations for end-user devices such as desktops, laptops and PDAs?
    d. If no, is a security plan being developed?

47. Has the system had a FISMA-based security assessment conducted by an independent third-party?
    a. If yes, what is the date of the last assessment?
    b. If yes, has a copy of the assessment report been provided to GTA Enterprise Information Security?

48. Has the business/data owner knowingly accepted the risk and granted an Authority/Approval to Operate for this system? (Y/N/Unk) If yes, provide date:

49. Does the system have a formal documented disaster recovery plan? (Y/N/InDev)
    a. If yes, what is the DR Plan date? (date last reviewed or updated, and approved)
    b. Has the DR Plan been tested? (Y/N)
    c. If yes, what is the date of the last test?

50. Who is the service provider for this system*?
    a. Agency (self provided) [ ]
    b. Enterprise Operating Vendors [ ]
    c. Third Party [ ] insert name _____

NOTE: If your answer is (a) or (c) for the above question, please answer questions 51 through 54 Otherwise this information will be provided by GTA.

51. Provide the number of agency full-time equivalent personnel (FTE) supporting this system.

52. Provide the number of contractor FTE supporting this system.

53. What is the total FY infrastructure expenditure for this system?

54. If you answered “Third Party” for Q. 50 on service provider, is the third party responsible for the equipment and equipment refresh?
    Otherwise, provide the quantity, general age and depreciated value of the system’s technology assets.

Technology Asset	**Quantity**	**Quantity older than 5 years**	**Depreciated Value ($)**
Windows Servers			
Mainframes			
UNIX Servers			
Desktop Workstations			
Laptops			
Wireless Devices (PDAs)			
Network devices			
Other (describe)			

Appendix - 3: Business Application Inventory

Agencies shall provide/update the following information for EACH business application owned by the agency

55. Provide the name of the business application.

56. Provide the application's short name*.

57. Who is the application business owner? (Name and contact info)

58. If applicable, provide the program code or subprogram name (PeopleSoft financial code).

59. Describe the purpose/business function for the application.

60. How essential is this application to the agency's core business?
    a. Mission Critical / Major Application
    b. Important
    c. General Support / Minor Application

61. Is this application covered by a security plan*?
    a. If yes, provide the name of the plan
    b. If no, is a plan in development?

62. Has the business/data owner knowingly accepted the risk and granted an Authority/Approval to Operate for this system?
    If yes, provide date.

63. What is the date the application was commissioned (start date)?

64. What is the expected life of the application (total number of years)?

65. Is there an upgrade planned for this budget year*?

66. What is the source of application software
    a. Custom Coded (state in-house or contract)
    b. COTS (product name / describe)
    c. Transfer
    d. Outsourced
    e. Other (describe)

67. What is the application support model*?
    a. In-house (self provider)
    b. Vendor supported (name)
    c. Enterprise Operating Vendors
    d. Other Outsourced Third Party (name)

68. What is the hardware platform and operating system hosting the application?
    a. Mainframe (type and OS)
    b. Midrange (type and OS)
    c. Windows (type and OS)
    d. Unix (type and OS)
    e. Desktop (type and OS)
    f. Other (describe)

69. What is the primary data service or data tier (usually a database) used?
    a. SQL
    b. Oracle
    c. DB2/UDB
    d. Access
    e. Sybase
    f. Lotus Notes
    g. IMS
    h. Informix
    i. DB2/IMS DB
    j. DB2/DLI
    k. DB2/VSAM
    l. Excel
    m. Multiple
    n. Other (explain)

70. What is the application architecture*?
    a. Monolithic Legacy
    b. Service Oriented/Web
    c. Client/Server
    d. Mobile Device
    e. N-tier -.NET
    f. N-tier – J2EE
    g. Hybrid
    h. Other

71. What type of processing does this application use*?
    a. Batch
    b. Interactive
    c. Batch & Interactive

72. What are the data sources for this application*?
    a. User input
    b. Live interfaces to other systems
    c. Batch feeds from other systems
    d. Other (explain)

73. Provide the number of users that use this application.

74. What type of business users does this application support*?
    a. Internal Agency
    b. Other GA state agencies
    c. Federal partners
    d. Local Government
    e. Businesses
    f. Citizens

75. Has a Customer Satisfaction survey been done this FY for this application*?

76. Provide the number of agency FTEs supporting this application.

77. Provide the number of contractor FTEs supporting this application.

78. What is the total YTD (FY2010) expenditure for operating this application?

79. What is the total FY budget (FY2011) for this application*?

80. What are the Top Risks/Challenges for this application*?
    - Complexity of Technology
    - Performance Goals
    - Business Objectives
    - Strategic Goals
    - Funding for support
    - Support personnel
    - Processes or business rules
    - Regulatory or legislative changes
    - Political environment
    - Leadership or ownership changes
    - Other

Appendix - 4: Project Portfolio

Each agency shall report on their Project Portfolio:

81. What is the project name?

82. Provide the project short name*.

83. Who is the Project Manager*?

84. Describe the project purpose.

85. Select the last Stage Gate Review completed*
    a. Concept
    b. Initiation
    c. Planning
    d. Requirements Analysis
    e. Design
    f. Development
    g. Test
    h. Transition
    i. Operations and maintenance
    j. Disposition

86. Provide the date of the last Stage Gate Review*

87. Select the review result for your last Stage Gate Review*:
    a. Pass
    b. Pass With Conditions
    c. Fail

88. Provide the project's planned start date.

89. Provide the project's actual start date*.

90. Provide the project's planned finish date*.

91. If actually finished, what was the actual finish date*?

92. Agency's priority for this project?
    a) High
    b) Moderate
    c) Low

93. Complete the following table concerning project budget and expenditures*.

	This FY	Next FY	Following FY
State Funds Budgeted			
Non-State Funds Budgeted			
Planned To-date Spend			
Actual To-date Spend			
Planned Work Accomplished			

94. What is the estimated spend at completion of the project?

* New for FY 2010.